

(FILE 'HOME' ENTERED AT 13:18:07 ON 14 AUG 1998)

L1 FILE 'WPIDS' ENTERED AT 13:18:17 ON 14 AUG 1998  
6 S MACRO# (5A) (VIRUS? OR INFECT?)

L2 FILE 'INSPEC' ENTERED AT 13:21:41 ON 14 AUG 1998  
30 S L1

L3 FILE 'COMPUSCIENCE' ENTERED AT 13:33:01 ON 14 AUG 1998  
0 S L1

L1 ANSWER 1 OF 6 WPIDS COPYRIGHT 1998 DERWENT INFORMATION LTD  
AN 98-240301 [21] WPIDS  
DNN N98-190046

TI Virus detection method for removal of **viruses** in  
**macros** - in which file is targetted for virus detection  
according to configuration settings of **macro virus**  
detection module, and copied into data buffer for analysis.

DC T01

IN CHEN, E Y; CHI, L M; DENG, M M; RO, J T

PA (TREN-N) TREND MICRO INC

CYC 24

PI WO 9814872 A1 980409 (9821)\* EN 50 pp G06F011-00  
RW: AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE  
W: AU BR CA CN IL JP NO

ADT WO 9814872 A1 WO 97-US16675 970929

PRAI US 96-724949 961002

IC ICM G06F011-00

AB WO 9814872 A UPAB: 980528

*copy it*  
The method for detection and removal of **macros** involves  
using a **virus** detection module (206) which determines  
(302) whether a targeted file includes a macro, and where the macro  
is found, locates and decodes (302) it to produce a decoded macro.  
The decoded macro is accessed and scanned (304) to determine whether  
it contains any viruses.

A macro treating module (310) locates suspect instructions in  
the decoded macro using comparison data for detecting unknown  
**macro viruses**, which are removed to produce a  
treated macro. A file correcting module (310) accesses a targeted  
file with an **infected macro** and replaces the  
**infected macro** with the treated **macro**  
produced by the treatment module (306).

USE - Detection and removal of **viruses** which reside  
in **macros**.

Dwg.3/9

FS EPI

FA AB; GI

MC EPI: T01-J20D

L1 ANSWER 2 OF 6 WPIDS COPYRIGHT 1998 DERWENT INFORMATION LTD  
AN 98-180353 [17] WPIDS  
DNN N98-142679

TI Virus checking method for computer word processing application -  
deactivating execution of automatic instruction sequences associated  
with opened file, and detecting and examining instruction sequences  
at file operation.

DC T01

IN BENEDIKT, R

PA (SIEI) SIEMENS AG

CYC 1

PI DE 19638143 A1 980319 (9817)\* 4 pp G06F012-16

ADT DE 19638143 A1 DE 96-19638143 960918

PRAI DE 96-19638143 960918

L2 ANSWER 4 OF 30 INSPEC COPYRIGHT 1998 IEE  
 AN 98:5875017 INSPEC DN C9805-6130S-042  
 TI **Macro virus** identification problems.  
 AU Bontchev, V. (FRISK Software Internat., Reykjavik, Iceland)  
 SO Computers & Security (1998) vol.17, no.1, p.69-89. 6 refs.  
 Published by: Elsevier  
 Price: CCCC 0167-4048/98/\$19.00  
 CODEN: CPSEDU ISSN: 0167-4048  
 SICI: 0167-4048(1998)17:1L.69:MVIP;1-R  
 DT Journal  
 TC Practical  
 CY United Kingdom  
 LA English  
 AB Computer **viruses** written in the **macro** programming language of the popular office applications like Microsoft Word have become extremely widespread. Unlike the MS-DOS **viruses** which are single entities, the **macro viruses** often consist of entire sets of several independent macros. This poses some interesting theoretical problems to the virus specific anti virus software that attempts to identify exactly the viruses it detects. Two viral sets of macros can have common subsets-or one of the sets could be a subset of the other. The paper deals with the problems caused by this, some of which are extremely difficult, if not impossible to solve. Emphasis is put on how the difficulties could be exploited by the virus writers and how the anti virus products should be improved in order to be made resistant to such attacks and to avoid damaging the user's documents when misidentifying the virus in it and attempting to remove the wrong virus variant.  
 CC C6130S Data security; C6140D High level languages; C0310D Computer installation management; C6110 Systems analysis and programming  
 CT COMPUTER VIRUSES; HIGH LEVEL LANGUAGES; MACROS; PROGRAMMING  
 ST **macro virus identification problems**; computer viruses; macro programming language; office applications; Microsoft Word; independent macros; virus specific anti virus software; virus writers; anti virus products; virus variant  
  
 L2 ANSWER 5 OF 30 INSPEC COPYRIGHT 1998 IEE  
 AN 98:5813802 INSPEC  
 TI Norman Virus Control v4.30 for Windows 95.  
 AU Jackson, K.  
 SO Virus Bulletin (Jan. 1998) p.25-7. 0 refs.  
 Published by: Virus Bulletin  
 Price: CCCC 0956-9979/98/\$0.00+2.50  
 CODEN: VBULE3 ISSN: 0956-9979  
 DT Journal  
 TC Practical; Product Review  
 CY United Kingdom  
 LA English  
 AB Norman Data Defense Systems alleges that the Norman Virus Control (NVC) virus scanner can now detect and remove all known **macro viruses**. It makes the same claim of its

memory-resident scanner. These are bold words, and I tried to test the product again on them. There are versions of NVC but this review only covers version 4.30 for standalone Windows 95. NVC only missed four samples of a single Excel virus and it detected all the other **macro viruses**. However, some of the ways in which NVC operates are, to put it mildly, quirky. The mode of operation is not wrong or inferior, it just does things in ways that are not initially clear. Once this is realized, NVC works very well, is very capable of detecting viruses (polymorphic detection is outstanding at 100%), and it scans quickly. It should prove to be a good buy.

CC D1060 Security

CT COMPUTER VIRUSES; GRAPHICAL USER INTERFACES; MICROCOMPUTER APPLICATIONS; PROGRAM TESTING; SOFTWARE REVIEWS; UTILITY PROGRAMS

ST Norman Virus Control v4.30 for Windows 95; Norman Data Defense Systems; virus scanner; **macro viruses**; memory-resident viruses; software testing; Excel; quirkiness; polymorphic detection

L2 ANSWER 6 OF 30 INSPEC COPYRIGHT 1998 IEE

AN 98:5813799 INSPEC

TI Inoculan AntiVirus v5.0 for Windows 95.

AU Jackson, K.

SO Virus Bulletin (Dec. 1997) p.13-16. 0 refs.  
Published by: Virus Bulletin  
Price: CCCC 0956-9979/97/\$0.00+2.50  
CODEN: VBULE3 ISSN: 0956-9979

DT Journal

TC Practical; Product Review

CY United Kingdom

LA English

AB Computer Associates claims its product is 'a full-featured Windows 95 application that detects and removes viruses'. In other words a scanner, and both on-demand and memory-resident components are provided. Inoculan's packaging claims '100% protection, 100% cure against all **macro viruses**', and 'Automatic Protection Against **Virus** Attack GUARANTEED'. The latter claim is already dead in the water-nothing provides guaranteed protection against virus attacks. Anyone who claims that their product does is either lying or does not understand the problem.

CC D1060 Security; D5000 Office automation - computing

CT COMPUTER VIRUSES; INTEGRATED SOFTWARE; PROTECTION; SOFTWARE REVIEWS

ST Computer Associates Inoculan AntiVirus v5.0 for Windows 95; virus removal; virus detection; scanner; memory-resident components; on-demand components; **macro viruses**; virus attack protection

L2 ANSWER 14 OF 30 INSPEC COPYRIGHT 1998 IEE

AN 97:5655531 INSPEC

TI Into the valley of DOS [DOS scanner benchmarking].

AU Crewe, P.

SO Virus Bulletin (July 1997) p.8-17. 0 refs.  
Published by: Virus Bulletin  
Price: CCCC 0956-9979/97/\$0.00+2.50  
CODEN: VBULE3 ISSN: 0956-9979

DT Journal

TC Practical; Product Review

CY United Kingdom

LA English

AB The following virus scanner software packages are compared: Alwil AVAST!, Anywhere Antivirus, Cheyenne InocuLAN, Command F-PROT, Cybec

VET, Data Fellows F-PROT, DialogueScience DrWeb, Dr. Solomons AVTK, EliaShim ViruSafe, ESaSS ThunderBYTE, H+BEDV AVE32B, H+BEDV AVSCAN, IBM Antivirus, Intel LANDesk, Iris antiVirus, KAMI AVP, Look Software Virus ALERT, McAfee VirusScan, Norman Virus Control, SafetyNet VirusNet, Sophos SWEEP, Stiller Integrity Master, Symantec Norton AntiVirus, Trend PC-cilin.

CC D1060 Security

CT COMPUTER VIRUSES; SOFTWARE REVIEWS

ST DOS scanner benchmarking; Sophos SWEEP; virus scanner software packages; Stiller Integrity Master; Alwil AVAST!; Symantec Norton AntiVirus; Anywhere Antivirus; Trend PC-cillin; Cheyenne Inoculan; anti virus developments; Command F-PROT; command line scanner; Cybec VET; **macro viruses**; Data Fellows F-PROT; DialogueScience DrWeb; Dr. Solomons AVTK; EliaShim ViruSafe; ESaSS ThunderBYTE; H+BEDV AVE32B; H+BEDV AVSCAN; IBM Antivirus; Intel LANDesk;; Iris antiVirus; KAMI AVP; Look Software Virus ALERT; McAfee VirusScan; Norman Virus Control; SafetyNet VirusNet

L2 ANSWER 17 OF 30 INSPEC COPYRIGHT 1998 IEE

AN 97:5499923 INSPEC

TI Virus ALERT.

AU Jackson, K.

SO Virus Bulletin (Jan. 1997) p.21-3. 0 refs.  
Published by: Virus Bulletin  
Price: CCCC 0956-9979/97/\$0.00+2.50  
CODEN: VBULE3 ISSN: 0956-9979

DT Journal

TC Practical; Product Review

CY United Kingdom

LA English

AB VirusALERT is a multifaceted package including a scanner, memory-resident anti-virus programs, disinfection features, and a disk recovery program. The author reviews its main components. The product was provided for review on four 1.44 MB floppy disks, two marked "**Virus** ALERT", one for **macro viruses**, and one marked "TESTER".

CC D1060 Security

CT COMPUTER VIRUSES; SOFTWARE REVIEWS; SYSTEM RECOVERY

ST Virus ALERT; multifaceted software package; virus scanner; memory-resident anti-virus programs; computer virus disinfection features; disk recovery program; floppy disks; **macro viruses** ; TESTER; 1.44 MB

PHP memory size 1.51E+06 Byte

L2 ANSWER 25 OF 30 INSPEC COPYRIGHT 1998 IEE

AN 96:5238813 INSPEC

TI PC pesticides [Windows 95 anti-virus software].

AU Howlett, D.

SO What Personal Computer (April 1996) no.81, p.124-6. 0 refs.  
Published by: EMAP Computing  
CODEN: WPCMFQ ISSN: 0956-5248  
SICI: 0956-5248(199604)81L:124:PWAV;1-T

DT Journal

TC Practical; Product Review

CY United Kingdom

LA English

AB Find out how to protect your PC against the 7000 known computer viruses with the latest Windows 95 ready software.

CC D5000 Office automation - computing; D1060 Security

CT COMPUTER VIRUSES; SOFTWARE REVIEWS

ST Windows 95 anti-virus software; PC pesticides; computer viruses; bug program; Trojan horse; Cyberspace; Word for Windows; **macro viruses**; Green Stripe; Boza; software packages; Sweep; Sophos; Norton Anti-Virus 95; configuration option; Dr Solomon's; McAfee Virus Scan; SMEG virus; VirusScan

IC ICM G06F012-16  
ICS G06F011-28; G06F017-21  
AB DE19638143 A UPAB: 980428

The method includes the steps starting a data processing application and deactivating an execution of automatic instruction sequences which may be associated with the file. A check or a query on the existence of such associated instruction sequences is performed at a file operation.

At detecting such sequence, a message is generated, which requests the execution of an instruction for processing the detected instruction sequence. The instruction sequence is processed, and depended on the result of the processing, the sequence may be deleted or executed by removing the deactivation.

USE - Esp. for detecting **macro-virus** in word editor, e.g. Winword, Excel, Windows applications.

ADVANTAGE - Improves protection against **viruses** implemented as word-processor **macros**.

Dwg.0/0

FS EPI  
FA AB  
MC EPI: T01-J20D

d his

(FILE 'USPAT' ENTERED AT 13:12:03 ON 14 AUG 1998)

L1 3 S (MACRO (3A) VIRUS##)

L2 0 S MACROVIRUS##

L3 3 S MACRO# (3A) VIRUS?

L4 59 S MACRO# (5A) (INFECT? OR AFFECT?)

L5 3 S L4 AND VIRUS?

L6 15 S L4 AND 395/CLAS

=>